

United States District Court

FOR THE
NORTHERN DISTRICT OF CALIFORNIA

VENUE: SAN FRANCISCO

FILED

Dec 13 2022

Mark B. Busby
CLERK, U.S. DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN FRANCISCO

UNITED STATES OF AMERICA,

V.

Miklos Daniel Brody

DEFENDANT(S).

SUPERSEDING INDICTMENT

18 U.S.C. § 1030(a)(2)(C) and (c)(2)(B) – Obtaining Information from a Protected Computer

18 U.S.C. § 1030(a)(5)(A) & (c)(4)(B)(i) - Intentional Damage to a Protected Computer

18 U.S.C. § 1001(a)(2) – False Statements to a Government Agency

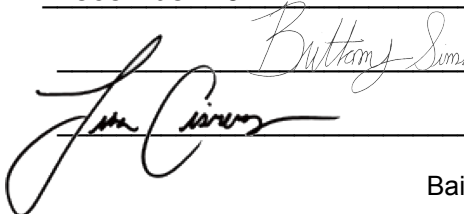
A true bill.

/s/ Foreperson of the Grand Jury

Foreman

Filed in open court this 13th day of

December 2022.


Brittany Sims, Clerk

Bail, \$ No Process


Hon. Lisa J. Cisneros, Magistrate Judge

FILED

Dec 13 2022

Mark B. Busby
CLERK, U.S. DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN FRANCISCO

STEPHANIE M. HINDS (CABN 154284)
United States Attorney

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN FRANCISCO DIVISION

UNITED STATES OF AMERICA,)	CASE NO. 3:22-cr-00168 WHO
)	
Plaintiff,)	<u>VIOLATIONS:</u>
)	18 U.S.C. §§ 1030(a)(2)(C) and (c)(2)(B) – Obtaining
v.)	Information from a Protected Computer;
)	18 U.S.C. §§ 1030(a)(5)(A) and (c)(4)(B)(i) –
MIKLOS DANIEL BRODY,)	Transmission of a Program, Information, Code, and
)	Command to Cause Damage to a Protected Computer;
Defendant.)	18 U.S.C. § 1001(a)(2) – False Statement to a
)	Government Agency;
)	18 U.S.C. §§ 982(a)(2)(B) and 1030(i) and (j) –
)	Forfeiture Allegation
)	
)	SAN FRANCISCO VENUE

SUPERSEDING INDICTMENT

The Grand Jury charges:

Introductory Allegations

At all times relevant to the Superseding Indictment, with all dates approximate and all date ranges approximate and inclusive:

1. First Republic Bank (“FRB”) was headquartered in San Francisco, California. FRB was a financial institution that offered personal banking, business banking, trust, and wealth management services. FRB had computer systems and networks, including a cloud engineering computer environment, that it used in its operation as a financial institution.

SUPERSEDING INDICTMENT

1 2. Miklos Daniel Brody was employed by FRB as a cloud engineer. After FRB received
2 alerts that Brody was violating the company's Information and Systems Appropriate Use Policy, he was
3 fired on March 11, 2020. He was told to bring his company-issued 2018 Apple 15" MacBook Pro
4 laptop to his meeting with FRB Human Resources on March 11, 2020, but he did not. Brody was
5 informed at that meeting that he had been fired and he was not eligible for re-hiring by FRB. His
6 employee badge was collected, he was given an exit package, and he was escorted out of the office at
7 approximately 4:33 p.m. on March 11, 2020.

8 3. After he was escorted out of FRB's office, Brody still had not returned the company's
9 MacBook. At approximately 6:30 p.m. on March 11, 2020 – after Brody was fired – he accessed FRB's
10 computer network without authorization. Access to FRB's computer network was possible only by
11 using a pre-registered device. To access FRB's system, he used his unique multi-factor authentication
12 ("MFA"), username, and password and signed in as "dbrody/adm_dbrody."

13 4. Once Brody accessed the FRB computer system, he had access to, among other things,
14 FRB's code repositories and cloud infrastructure, including in the "Devbox," "GitHub," and the
15 Terraform Enterprise.

16 5. While Brody was in FRB's computer environment on or about March 11 and 12, 2020,
17 malicious activity occurred in the network that caused substantial damage. The malicious activity began
18 around 7:55 p.m. on March 11, 2020. The damage included, but is not limited to: Brody deleted
19 numerous FRB GitHub repositories. Damage also included Brody shutting down service to Terraform
20 Enterprise ("TFE") around 1 a.m. on March 12, 2020; TFE is a system that Brody took the lead on while
21 working for FRB. Brody also ran a malicious script called "dar.sh," the purpose of which was to delete
22 computer logs.

23 6. While Brody was in the system, Brody opened sessions in the names of other employees,
24 including FRB employee A.A., using the "root" user. Code-related "taunts" were also left in the system
25 for A.A. For instance, using the root user, Brody stored a password titled "grockit.pem" in A.A.'s
26 DevBox. "Grok" means "to understand." "Grok" had been the basis of a prior work conversation in
27 which Brody's co-workers, including A.A., had taught Brody the meaning of the term because Brody
28 was unfamiliar with it. In the taunt, the term was misspelled ("grock" rather than "grok").

1 7. On or about the morning of March 12, 2020, and no later than approximately 11:30 a.m.,
2 after the bank discovered that damage had been caused, FRB terminated Brody's credentials. The
3 malicious activity ended after Brody's credentials were terminated.

4 8. FRB estimates the total cost of the damage to its system to be at least approximately
5 \$220,000. The damage included FRB's efforts to assess the damage and restore service – which was
6 made more difficult by the way in which Brody caused damage. For instance, after Brody deleted the
7 GitHub repositories, Brody tampered with back-up GitHub repositories, such that FRB could not easily
8 restore service on GitHub. This led to idle time for numerous FRB software engineers, who rely on
9 access to GitHub to work. Brody's efforts to cover his tracks – by, for instance, deleting user logs or
10 using the "root" user – further exacerbated efforts to assess the damage and restore service.

11 9. In the days and weeks following the network intrusion, Brody engaged in a series of
12 evasive and deceptive actions. For example, on March 13, 2020, the day after the intrusion ended and
13 his FRB credentials were deactivated, Brody added bookmarks to Internet websites with the titles "Need
14 to Remove Firmware Password," "Bypass Mac Firmware Password," and "Forgot a Mac Firmware
15 Password? Don't Panic, Here's What To Do." Bypassing a firmware password would have allowed
16 Brody to "wipe" (or delete information from) a computer.

17 10. Agents also found WhatsApp messages on Brody's cell phone from the evening of March
18 13, 2020 between Brody and a person with the screenname "Hackdude." In the exchange, Brody talked
19 to "Hackdude" about the price of bypassing firmware on a 2018 Macbook computer.

20 11. The next day, March 14, 2020, a YouTube video was bookmarked in Brody's Internet
21 history titled "How to Take Apart the 2018 15" Macbook Pro A1990."

22 12. Brody added further web bookmarks in late March 2020. On March 29, 2020, a
23 bookmark was added entitled "Unauthorized Computer Access by Former Employee – Protection of
24 Trade Secrets." The next day, bookmarks were added titled "Computer Fraud and Abuse Act No Help
25 to Employer Suing Employee Who Took Proprietary Business Info," and "key-issues-incomputer-fraud-
26 andabuse." This was nearly one year before any charges were filed against Brody.

27 13. On March 19, 2020, Brody filed a police report with San Francisco Police Department
28 claiming his Apple MacBook Pro computer, along with some personal items including four keys on a

“Route 66” keychain and a black North Face jacket, had been stolen. The police report claimed the items had been stolen on March 16, 2020, while he was working out at a 24 Hour Fitness near 1850 Ocean Avenue in San Francisco. He later told FRB that his work MacBook had been stolen. Brody reaffirmed these allegations – including the date of the theft, that he was working out at the time of the theft, and that his FRB work computer (a Macbook), keys on a Route 66 keychain, and black North Face jacket had been stolen at the same time from his car – to special agents with the U.S. Secret Service during a post-arrest interview on March 16, 2021. Brody’s statements to U.S. Secret Service were false. Member records from 24 Hour Fitness do not show he worked out there on March 16, 2020; they instead show he was last there on March 7, 2020. The 24 Hour Fitness near 1850 Ocean Avenue was also closed due to COVID-19 as of March 16, 2020. Furthermore, during a subsequent search of Brody’s apartment on March 16, 2021, agents found a Route 66 keychain containing four keys and a black North Face jacket; both items matched the description of personal items that Brody claimed were stolen on March 16, 2020. In instant message conversations with his parents soon after the network intrusion and before filing his police report, Brody discussed how to approach the laptop and asked his parents advice on where he should put the laptop while he made the report to the police. The MacBook Brody claimed to be stolen, valued at \$2,799, was never returned to FRB or located by law enforcement. Brody knowingly and willfully made his false statements to the U.S. Secret Service on March 16, 2021 in order to mislead the U.S. Secret Service, a U.S. government executive agency, from finding the Macbook, which likely contained evidence of his unauthorized access and computer intrusion.

14. During their search of Brody’s apartment, agents also seized Brody’s personal computer. During a review of the personal computer’s contents, agents found FRB computer code that was taken from FRB’s GitHub. Records show that Brody had emailed this code to himself at approximately 11:06 a.m. on March 12, 2020—the day after he was fired. The value of that code exceeds \$5,000.

COUNT ONE: (18 U.S.C. §§ 1030(a)(2)(C), (c)(2)(B) – Obtaining Information from a Protected Computer)

15. The factual allegations contained in Paragraphs 1 through 14 are realleged and incorporated herein.

16. Beginning on or about March 11, 2020, and continuing through on or about March 12,

2020, in the Northern District of California, the defendant,

MIKLOS DANIEL BRODY,

intentionally accessed a protected computer without authorization and exceeded authorized access, and thereby obtained information from a protected computer, and committed the offense for purposes of commercial advantage and private financial gain, and the value of the information obtained exceeded \$5,000; specifically, defendant accessed First Republic Bank's computer network after being fired as an employee on March 11, 2020, and copied code belonging to the bank and worth over \$5,000 onto his personal computer, all in violation of Title 18, United States Code, Sections 1030(a)(2)(C) and (c)(2)(B).

COUNT TWO: (18 U.S.C. §§ 1030(a)(5)(A), (c)(4)(B)(i) – Intentional Transmission of a Program, Information, Code, and Command to Cause Damage to a Protected Computer)

17. The factual allegations contained in Paragraphs 1 through 14 are realleged and incorporated herein.

18. Beginning on or about March 11, 2020, and continuing through on or about March 12, 2020, in the Northern District of California, the defendant,

MIKLOS DANIEL BRODY,

knowingly caused the transmission of a program, information, code, and command, and, as a result of such conduct, intentionally caused damage without authorization to a protected computer, to wit, the defendant knowingly transmitted a program, information, code and command to the First Republic Bank computer system, which includes computers used in interstate and foreign commerce and communication, and, by such conduct, caused loss to one or more persons during a one-year period aggregating at least \$5,000 in value, all in violation of Title 18, United States Code, Sections 1030(a)(5)(A) and (c)(4)(B)(i).

COUNT THREE: (18 U.S.C. § 1001(a)(2) – False Statement to a Government Agency)

19. The factual allegations contained in Paragraphs 1 through 14 are realleged and incorporated herein.

20. On or about March 16, 2021, in the Northern District of California, the defendant,

MIKLOS DANIEL BRODY,

did willfully and knowingly make materially false, fictitious, and fraudulent statements and

representations in a matter within the jurisdiction of the executive branch of the Government of the United States by stating to U.S. Secret Service special agents investigating the allegations and crimes described in paragraphs 1 through 18 above that his police report made to San Francisco Police Department on March 19, 2020 was true and that, as documented in his March 19, 2020 police report, an Apple Macbook computer, owned by First Republic Bank, was stolen from his car on March 16, 2020 while he was at the gym. These statements and representations were false because, as BRODY then and there knew, his March 19, 2020 police report to San Francisco Police Department was false, and the First Republic Bank Apple Macbook computer was not stolen on March 16, 2020 from his car while he was at the gym. All in violation of Title 18, United States Code, Section 1001(a)(2).

FORFEITURE ALLEGATION: (18 U.S.C. §§ 982(a)(2)(B) and 1030(i) and (j))

21. The allegations contained in this Superseding Indictment are re-alleged and incorporated by reference for the purpose of alleging forfeiture pursuant to Title 18, United States Code, Sections 982(a)(2)(b) and 1030(i) and (j).

22. Upon conviction for the offenses set forth in Counts One and Two of this Superseding Indictment in violation of Title 18, United States Code, Section 1030(a), the defendant,

MIKLOS DANIEL BRODY,

shall forfeit to the United States, pursuant to Title 18, United States Code, Sections 982(a)(2)(b) and 1030(i) and (j), any personal property used or intended to be used to commit or to facilitate the commission of said violation or a conspiracy to violate said provision, and any property, real or personal, which constitutes or is derived from proceeds traceable to the offenses, including, but not limited to, a sum of money equal to the total amount of proceeds defendant obtained or derived, directly or indirectly, from the violation, or the value of the property used to commit or to facilitate the commission of said violation.

23. If any of the property described above, as a result of any act or omission of the defendant:

- a. cannot be located upon exercise of due diligence;
- b. has been transferred or sold to, or deposited with, a third party;
- c. has been placed beyond the jurisdiction of the court;
- d. has been substantially diminished in value; or

e. has been commingled with other property which cannot be divided without difficulty,

the United States of America shall be entitled to forfeiture of substitute property pursuant to Title 21, United States Code, Section 853(p), as incorporated by Title 18, United States Code, Section 1030(i)(2). All pursuant to Title 18, United States Code, Sections 982(a)(2)(B) and 1030, and Federal Rule of Criminal Procedure 32.2.

DATED: December 13, 2022

A TRUE BILL.

/s/ Foreperson
FOREPERSON

STEPHANIE M. HINDS
United States Attorney

/s/
LAUREN M. HARDING
GEORGE O. HAGEMAN
Assistant United States Attorneys